



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 04 June 2004

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- United Press International reports Chevron has become the third major gas company to sell tainted gasoline in Florida. (See item [4](#))
- The Associated Press reports two Texas tanker trucks carrying propane, stolen over the Memorial Day weekend, have been located; but the New Jersey gasoline tanker stolen in mid-April remains missing. (See item [13](#))
- InternetNews reports researchers warn that a security bypass flaw in a popular wireless broadband router shipped by Cisco's Linksys unit could give malicious hackers administrative access to vulnerable devices. (See item [35](#))
- The Scotsman reports atomic experts warn that a rise in the level of smuggling of radioactive material has increased the risk of a dirty bomb attack by terrorists. (See item [36](#))

### DHS/IAIP Update *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [General](#); [DHS/IAIP Web Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels:** Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 03, The Guardian (UK)* — **Once seen as an alarmist fear, an attack on key Saudi oil terminal could destabilize west.** When Fadel Gheit first warned of his "nightmare scenario" that Saudi Arabia's main oil export terminal at Ras Tanura could be wiped out by terrorists, he was dismissed as an alarmist. As fears of upheaval in Saudi helped set world crude oil prices to

21-year highs of \$42.45 per barrel, there were fewer willing to scoff at Gheit. "I cannot think of any more logical target for terrorists. It [Ras Tanura] is the nerve center for the Saudi oil trade but also for global exports. Saudi Arabia is the linchpin for world crude supplies, a key to setting prices and yet sitting on a political tinderbox due to internal dissent and having trouble securing itself against terrorism. An assault on Ras Tanura is very serious. **As much as 80% of the near 9m barrels of oil a day pumped out by Saudi is believed to end up being piped from fields such as Ghawar to Ras Tanura in the Gulf to be loaded on to supertankers bound for the west.**

Source: <http://www.guardian.co.uk/international/story/0,3604,1230112,00.html>

2. *June 03, Associated Press* — **Nuclear plants may count fuel rods. About a dozen nuclear power plants are being asked to inventory their fuel rods, following the loss of some rods at plants in Connecticut and Vermont. There is no evidence the rods got into the hands of terrorists, investigations found, but nuclear power regulators want the inventory to get a better idea how spent fuel is managed.** The nationwide review "is being done on a one-time basis to make sure plants have good control over what's in their spent fuel pools," said Neil Sheehan, spokesperson for the U.S. Nuclear Regulatory Commission. "There is an even higher sensitivity to properly safeguard this material post 9/11." The inventory will be done in three phases. First, power plant owners and federal inspectors must determine whether any fuel rods have ever been removed from their usual storage assemblies and placed in other containers. Plant operators must account for those fuel rods through record-keeping or other means. Then, they may have to do an intensive inspection to locate and account for the waste.

Source: <http://www.newsday.com/news/local/wire/ny-bc-ct--nuclearfuel rods0603jun03.0,7443788.story?coll=ny-ap-regional-wire>

3. *June 03, Associated Press* — **Tens of thousands have no power in Louisiana.** Nearly 70,000 homes in northwest Louisiana were without power on Wednesday, June 2, following a fourth night of rain and high winds. Power company AEP SWEPCO says it will bring in reinforcement crews from Arkansas and Texas to help restore power. Pierre-Bossier mall in Bossier City, LA, was evacuated after part of the mall's roof was ripped off. **AEP SWEPCO spokesperson Kay Holt says it might take into the weekend for all the customers to be restored.**

Source: <http://www.katc.com/Global/story.asp?S=1915521&nav=EyAzNd7Z>

4. *June 03, United Press International* — **More tainted gas found in Florida. Chevron became the third major gas company to sell tainted gasoline in Florida recently. Shell and Texaco stopped sales in many areas because of high sulfur content in gasoline sold by Motiva Enterprises in Houston, TX.** Sulfur corrodes the silver inside fuel gauges, causing them to malfunction. **Chevron said as many as 94 of its gas stations in the Tampa, FL, area received the tainted gasoline.** Chevron said those stations have been selling untainted gas since Friday, May 28. The gas had been shipped into terminals at Tampa and Port Everglades at Fort Lauderdale in Florida. Gas companies and the Florida Department of Agriculture and Consumer Services said they are investigating the situation.

Source: <http://washingtontimes.com/upi-breaking/20040603-111011-1907 r.htm>

5. *June 03, Bloomberg* — **Crude oil tumbles after reports show U.S. inventories gained.** Crude oil futures declined with gasoline prices after U.S. reports showed oil and motor fuel supplies

gained recently. **Nationwide gasoline supplies jumped 2.8 million barrels to 200.7 million in the week ended May 28, the American Petroleum Institute said. The Department of Energy (DOE) earlier reported gasoline reserves rose 1.3 million barrels to 204.3 million. High imports and domestic production helped boost gasoline stockpiles.** U.S. oil inventories gained as shipments climbed near record levels. U.S. crude oil supplies increased by a larger-than-expected 2.8 million barrels to 301.7 million in the week ended May 28, 4.4 percent higher than a year ago, based on DOE data. Imports rose 2 percent to 10.7 million barrels a day, the highest since September when shipments reached a record. Also, the Organization of Petroleum Exporting Countries (OPEC) agreed to raise quotas by 2 million barrels a day, or 8.5 percent, an amount less than what some ministers said was needed to prevent high prices from curbing global economic growth. OPEC, source of more than a third of the world's oil, said it may boost the limit by another 500,000 barrels a day in August, said Saudi Arabia's oil minister Ali al-Naimi.

Source: <http://quote.bloomberg.com/apps/news?pid=10000103&sid=aeYBvOJaAOEQ&refer=us>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

### **6. *June 03, Associated Press* — Evacuations after chemical leak in North Carolina.**

**Neighborhoods were evacuated as a precaution Thursday, June 3, following a chemical leak at a fertilizer plant in Lenoir, NC.** There were no injuries, but about 20 people — including five workers, several firefighters and residents — had to be decontaminated after being exposed to hydrogen sulfide, Lenoir Fire Chief Ken Briscoe said. Lenoir Police Department members complained about a pungent smell near downtown Thursday morning, Briscoe said. **It was quickly determined that there had been a small release of hydrogen sulfide from the Marlin Co. Inc., plant, where workers were mixing chemicals to make fertilizer, he added.** "We have evacuated everyone with a half-mile radius of the plant," said Briscoe, who expected that residents would be allowed to go home by mid-afternoon. Marlin Co. owner Marty Waters said the situation appeared under control. "We are monitoring the air and at this point it (the leak) is going down steadily," he said.

Source: [http://abclocal.go.com/wtvd/news/060304\\_APstate\\_chemicalleak.html](http://abclocal.go.com/wtvd/news/060304_APstate_chemicalleak.html)

[[Return to top](#)]

## **Defense Industrial Base Sector**

### **7. *June 02, Associated Press* — Carrier demonstrates new deployment plan.** The aircraft carrier USS Harry S. Truman set sail Wednesday, June 2, in a test of the Navy's ability to have seven of its 12 carriers away from port at the same time, a major shift away from the customary deployment of the fleet. A second Norfolk, VA-based carrier, the USS Enterprise, was expected to leave Thursday, June 3, to participate in the exercise, dubbed "Summer Pulse 04." **The exercise continues through August with seven carriers and will include allied forces from around the world, officials said. It is the first exercise of the Navy's new Fleet Response Plan, in which ships will move away from regularly scheduled, six-month**

**deployments and instead be prepared to leave as world events demand.** The Navy wants to be able to send six carrier strike groups in less than 30 days to handle crises anywhere in the world, while having two more carrier strike groups ready to sail within three months to reinforce or rotate with those forces.

Source: [http://abcnews.go.com/wire/US/ap20040602\\_1229.html](http://abcnews.go.com/wire/US/ap20040602_1229.html)

8. *June 02, Government Computer News* — **DoD begins cross-credentialing pilot.** The Department of Defense (DoD) is sponsoring a pilot program to test interoperability of government and private-sector identification credentials. The Defense Manpower Data Center and six defense contractors participating in the summer-long pilot will use a central DoD broker to authenticate each other's credentials. The program is an effort of the Defense Cross-credentialing Identification System and the Federated Electronic Government Coalition, a private-sector organization promoting electronic transactions with the government. **The goal is to enable contractors to validate and accept DoD's Common Access Card at company facilities, and for DoD to validate private-sector IDs at military facilities. Thousands of contractors enter DoD facilities each day using company-issued IDs. "Right now we have to take their word for it" that the ID is valid,** according to Bill Boggess, chief of the DMDC's access and authentication technology division. "The system allows each party to hold their own data," Boggess said. There is no central ID database. "At this level we're talking about Web services to achieve this," he continued.

Source: [http://www.gcn.com/vol1\\_no1/daily-updates/26077-1.html](http://www.gcn.com/vol1_no1/daily-updates/26077-1.html)

9. *May 13, General Accounting Office* — **GAO-04-519: Nonproliferation: Further Improvements Needed in U.S. Efforts to Counter Threats from Man- Portable Air Defense Systems (Report).** The proliferation of man-portable air defense systems (MANPADS) has been of growing concern to the United States and other governments. The United States is pursuing a wide variety of activities internationally and domestically to address this threat. **General Accounting Office (GAO) was asked to assess efforts by (1) the State Department to control global proliferation of MANPADS, (2) the Department of Defense (DoD) to monitor end-use of U.S.-exported Stingers, and (3) the Department of Homeland Security (DHS) to develop technical countermeasures to minimize the threat of a MANPADS attack.** The Secretary of State should develop a strategy to work within multilateral forums to establish mechanisms for assessing foreign governments' implementation of their commitments to reduce MANPADS proliferation. The Secretary of Defense should (1) establish standardized requirements for keeping Stinger missile records; (2) create an electronic database to consolidate all DoD records for Stinger missile systems sold overseas and track the worldwide Stinger inventory; and (3) direct that standardized procedures for conducting Stinger inspections be issued. State and DoD concurred with our recommendations. Highlight:

<http://www.gao.gov/highlights/d04519high.pdf>

Source: <http://www.gao.gov/new.items/d04519.pdf>

[[Return to top](#)]

## **Banking and Finance Sector**

10. *June 03, General Accounting Office* — **GAO-04-833T: Anti-Money Laundering: Issues Concerning Depository Institution Regulatory Oversight (Testimony).** The U.S.

government's framework for preventing, detecting, and prosecuting money laundering has been expanding through additional pieces of legislation since its inception in 1970 with the Bank Secrecy Act (BSA). The purpose of the BSA is to prevent financial institutions from being used as intermediaries for the transfer or deposit of money derived from criminal activity and to provide a paper trail for law enforcement agencies in their investigations of possible money laundering. The most recent changes arose in October 2001 with the passage of the USA PATRIOT Act, which, among other things, extends antimoney laundering (AML) requirements to other financial service providers previously not covered under the BSA. **General Accounting Office (GAO) was asked to testify on its previous work and the ongoing work it is doing for the Senate Committee on Banking, Housing, and Urban Affairs on the depository institution regulators' BSA examination and enforcement process.** Highlights: <http://www.gao.gov/highlights/d048333thigh.pdf>  
Source: <http://www.gao.gov/new.items/d048333t.pdf>

11. *June 02, Reuters* — **U.S. agency concedes shortfall in supervising Riggs.** A U.S. bank regulatory agency acknowledged on Wednesday, June 2, it failed to act quickly and forcefully enough in response to warning flags that Riggs Bank was not complying with anti-money-laundering laws. Riggs agreed to pay a \$25 million penalty May 13 amid allegations by regulators it failed to properly report and track potentially suspicious transactions as required under the Bank Secrecy Act, which is meant to prevent money-laundering. **Lawmakers have questioned the Office of the Comptroller of the Currency's (OCC) response in the Riggs case and have suggested strengthening bank oversight to provide better protection against illegal money transfers or the potential use of money for any terrorist activities.** "While errors of judgment were made on Riggs, Riggs was an anomaly and that system as a whole presently functions very well," Daniel Stipano, deputy chief counsel of OCC, said. However, lawmakers disagreed, saying the regulator's slowness to act raises concerns about the government's capacity to prevent money-laundering.  
Source: [http://biz.yahoo.com/rc/040602/financial\\_banks\\_moneylaundering\\_3.html](http://biz.yahoo.com/rc/040602/financial_banks_moneylaundering_3.html)

[[Return to top](#)]

## **Transportation Sector**

12. *June 03, CNN* — **Air travel chaos hits Britain. Thousands of air travelers were caught up in a chaos of queues and delays after a computer failure in one of Britain's main air traffic control centers grounded many of the country's flights and cancelled others.** Flights to and from British airports resumed later Thursday, June 3, a spokesperson for National Air Traffic Services (NATS) said. "We are fully operational now. We are now dealing with the backlog of delays. It affected all airports in England and Wales," the spokesperson told Reuters. **"It was a problem with the flight data processing system. We are looking into that now. It was not sabotage,"** he added. Reuters reported delays of around three hours at London's Heathrow airport. Officials said they do not suspect foul play, but the delays are expected to cost airlines millions of dollars, Muriel said. Thursday's computer failure is the latest in a series of difficulties that has hit Britain's air traffic services in recent years.  
Source: <http://www.cnn.com/2004/WORLD/europe/06/03/britain.flight/index.html>

13.



*June 03, Associated Press* — **Propane tankers stolen from San Antonio found; no word on missing New Jersey tanker.** Two tanker trucks carrying 5,600 gallons of propane that were stolen over the Memorial Day weekend in San Antonio were located on June 2, on a road near Laredo, TX. Both vehicles are owned by Ferrellgas. FBI spokesperson Rene Salinas said there's a big market for propane in Mexico, and FBI agent Patrick Patterson told NBC before the September 11 terrorist attacks, concern would not have been great about the missing tankers. **Authorities also are investigating the theft of 15 gas canisters from an ambulance supply company.** However, it's not believed the thefts were connected. **On a related matter, authorities announced June 2 that they have no new information on the New Jersey gasoline tanker truck that has been missing since mid-April.** "We still have no news. We're continuing to investigate," said Jerri Williams, spokesperson for the FBI in Philadelphia. This truck is a "refurbished" 1996 Pennsauken truck with TK transport in large green letters on the side.

Source: [http://www.thetrucker.com/stories/06\\_04/0603\\_stolen\\_tanker.html](http://www.thetrucker.com/stories/06_04/0603_stolen_tanker.html)

14. *June 03, Associated Press* — **Government plans new rail security experiments.** The government plans two new experiments to determine the feasibility of security checks for rail passengers and their bags. **Beginning next week, the Transportation Security Administration will screen checked baggage that goes onto the five long-distance Amtrak trains that depart Washington's Union Station every weekday.** Screeners will use some combination of X-ray machines, bomb-sniffing dogs and handheld wands that can sense minute traces of explosives. **Next month, the TSA will screen passengers as they board trains. Plans call for people to enter through the rear car, where they'll be checked for explosives before moving forward to their seats.** It's expected screeners will use an X-ray machine for carry-on baggage and a portal that "sniffs" the air around a person for explosive residue. It isn't yet clear which trains will be selected for the passenger test. Easy access to trains and train platforms make them vulnerable to terrorist attacks. The FBI and the Homeland Security Department have warned that terrorists might strike trains and buses in major U.S. cities using bombs concealed in bags or luggage. Though it's unlikely that TSA would ever try to screen all passengers and all bags on all railroads — let alone transit systems — the agency could later use the techniques it's testing when there's a specific threat or for special events.

Source: <http://www.phillyburbs.com/pb-dyn/news/27-06032004-310934.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

15. *June 03, DM News* — **Senate committee approves postal reform bill.** The Senate Committee on Governmental Affairs unanimously approved the Postal Accountability and Enhancement Act Wednesday, June 2. The bill now moves to the full Senate. The bill is similar to H.R. 4341, which passed out of committee May 12. The full House is to take up the bill by the end of June. **Among other elements, S. 2468 would repeal a provision requiring that money owed to the U.S. Postal Service (USPS) because of an overpayment into the Civil Service Retirement System fund be held in an escrow account. This repeal essentially would free up \$78 billion over 60 years.** The USPS has said it would use this money to pay off debt to the Department of Treasury, fund its healthcare liabilities and mitigate rate increases. If the money isn't released, the USPS said, it will be forced to seek a double-digit rate increase in 2006. The

bill also would return responsibility for funding pension benefits relating to the military service of postal retirees — a \$27 billion obligation — to the Department of Treasury. No other federal agency is required to make this payment.

Source: [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article\\_id=28213](http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=28213)

[\[Return to top\]](#)

## **Agriculture Sector**

16. *June 03, Dow Jones Newswires* — **More chickens killed in Texas county where bird flu was found.** A second flock of Texas breeder chickens was destroyed after tests showed some of the birds were infected with avian flu, officials said Wednesday, June 2. **The 24,000 chickens owned by poultry producer Pilgrim's Pride were at a farm about five miles from the east Texas farm where bird flu was detected last week, state animal health officials said.** "We did this as a prudent, pre-emptive step," said Sondra Fowler, a spokesperson for Pilgrim's Pride. The birds were killed Saturday, May 29, a day after another flock of 24,000 chickens was killed. The outbreak is the second in Texas this year, but officials said they are unrelated. In February, the virus was reported at a farm near Gonzales, east of San Antonio. More than 9,000 chickens were destroyed and several countries banned Texas poultry.

Source: [http://www.agprofessional.com/show\\_story.php?id=25443](http://www.agprofessional.com/show_story.php?id=25443)

17. *June 03, Associated Press* — **Salmon disease outbreak alarms officials. California fisheries officials are worried that a parasite killing young salmon and steelhead migrating down the Klamath River to the ocean could kill hundreds of thousands of the fish in coming weeks.** Young chinook, coho, and steelhead infected with the parasite *Ceratomyxa shasta* began showing up in traps that sample the annual migration around May 1, said senior California Department of Fish and Game fisheries biologist Neil Manji. The parasite is found up and down the river, but the cause of the outbreak remains unknown. The first sick fish were spotted in the trap farthest upriver. Over the course of the past month, up to 80 percent of the fish in traps showed symptoms of the parasite, and 50 percent were dead, Manji said. It is unclear if the same proportion can be transferred to the millions of fish in the river. The numbers raised concerns of a repeat of a 2000 fish kill that left an estimated 300,000 young salmon and steelhead dead from the same parasite and a fungus that attacks the gills, Manji said.

Source: <http://www.nytimes.com/aponline/business/AP-Farm-Scene.html>

18. *June 03, Associated Press* — **Researchers look for new plant strains to resist disease. Two University of Idaho researchers are trying to develop new kinds of wheat and barley that can resist an evolving fungus that stunts plant growth.** "This year doesn't seem to be as bad as last year, but stripe rust is certainly developing in the western parts of the Pacific Northwest and could move further east," said Ed Souza, a plant breeder at the university's Aberdeen Research and Extension Center in eastern Idaho. **Stripe rust has been a problem for wheat in Idaho since the 1960s and for barley the last decade.** Over the past generation resistance to the fungus has been bred into various lines of wheat. But Souza and support scientist Mary Guttieri said resistance has been focused too narrowly so that as the rust evolves into new strains, it can again successfully attack grains that has been resistant in the past. "What's perplexing is why it's become so much worse in the last four or five years," Souza said. During the winter, Souza and Guttieri tested several hundred lines of wheat in California and settled on

50 for further testing this summer. Included are 10 so-called slow-rusting lines that are not completely resistant but should fend off stripe rust for a much longer time than clean resistant types of wheat.

Source: [http://seattlepi.nwsource.com/local/aplocal\\_story.asp?category=6420&slug=ID%20Grain%20Rust](http://seattlepi.nwsource.com/local/aplocal_story.asp?category=6420&slug=ID%20Grain%20Rust)

[\[Return to top\]](#)

## **Food Sector**

### **19. *June 03, The Herald (United Kingdom)* — Warning over bacteria in dried baby food.**

Parents were given a fresh warning about baby food Wednesday, June 2, after a survey found some products contain potentially harmful bacteria. Researchers from Nottingham Trent University analyzed powdered infant formula, dried infant food and, milk powder from the UK, six other European countries, the U.S., South Korea, and South Africa. More than 200 samples from 110 different products were analyzed for the presence of various kinds of bacteria. **Of 102 newly purchased samples of powdered milk formula, three tested positive for the microbe enterobacter sakazakii — an organism which can cause meningitis in premature and weak babies with poor immune systems. Five of 49 samples of dried infant food, and three of 72 samples of dried milk powder also contained the bacteria.** A number of samples were also contaminated with other kinds of common infectious bacteria.

Source: <http://www.theherald.co.uk/news/17364.html>

### **20. *June 02, Food and Drug Administration* — FDA investigating illnesses associated with school lunches. The U.S. Food and Drug Administration (FDA), the Massachusetts Department of Public Health, and the U.S. Centers for Disease Control and Prevention are actively investigating what may have caused four outbreaks of illnesses in children related to meals served at several schools in Massachusetts beginning in May 2003, and occurring in a Revere, MA, school as recently as May of this year. Cases of illness have been reported among those who consumed school meals, with symptoms ranging from nausea, vomiting, diarrhea, stomach cramps, and dizziness. The onset of illness has usually begun within one hour of eating these meals, and usually lasts less than one day. In nearly every case, the meals involved contained tortillas produced by Del Rey Tortilleria, Inc. of Illinois, and distributed under the brand names Del Rey Tortilleria or Pan De Oro. Investigations and repeated laboratory analyses by FDA of tortillas and ingredients have not identified any particular contaminant as the vehicle for these illnesses.**

Source: <http://www.fda.gov/bbs/topics/news/2004/NEW01074.html>

[\[Return to top\]](#)

## **Water Sector**

### **21. *June 03, Government Technology* — Maine sells water test kits online. To encourage citizens to test their private water supplies, Maine's Department of Human Services is now selling water test kits through the state's official Website, <http://www.govtech.net/news/www.Maine.gov>. Consumers can choose from a variety of water**



test kit providers and certified laboratories that are listed on the Web site. Maine's Department of Human Services Commissioner John R. Nicholas noted that the Internet order form should increase the number of wells being tested, which will lead to better health in the long run.

"Almost half of our population gets its drinking water from private wells, and few of them are routinely tested. Water test kits are an important way to ensure water quality, and online access will make it easier for more of our citizens to use an important tool that can help them safeguard their health and that of their families," Nicholas said.

Source: <http://www.govtech.net/news/news.php?id=90477>

[[Return to top](#)]

## **Public Health Sector**

22. *June 03, Associated Press* — **Cruise passengers stricken by stomach virus. Nearly 350 passengers and crew aboard a Princess Cruises ship in southeast Alaska fell ill with a virus this week, cruise line officials said.** As of Wednesday, June 2, 308 passengers and 40 crew members aboard the Island Princess complained of Norwalk virus-like symptoms. Altogether, 2,018 passengers and 896 crew members were making the weeklong voyage from Vancouver, British Columbia, to Whittier, AK. Onboard testing confirmed the presence of the norovirus, which includes Norwalk and Norwalk-like viruses. The virus can cause diarrhea, stomach pain, and vomiting for 24 to 48 hours. The U.S. Centers for Disease Control and Prevention is investigating.

Source: <http://www.cnn.com/2004/TRAVEL/06/03/alaska.sick.ship.ap/>

23. *June 03, PR Newswire* — **Panacos Pharmaceuticals to merge With V.I. Technologies.** Panacos Pharmaceuticals Inc. Thursday, June 3, announced that it has entered into a definitive merger agreement with V.I. Technologies, Inc. (Vitex). Vitex is a public company, based in Watertown, MA that is developing innovative anti-infective technologies to enhance blood safety. **The merged company will have a strong pipeline of products for serious infectious diseases.** The combined Company which will use the V.I. Technologies and Vitex names. **Vitex is developing products to improve the safety of the world's blood supply. Its proprietary technology inactivates a wide range of viruses, bacteria, and parasites, and has demonstrated its ability to remove prion proteins. Panacos is developing antiviral drugs with novel mechanisms of action.** Under the terms of the transaction, Vitex will issue 25 million common shares in exchange for all outstanding Panacos shares upon the close of the transaction. The transaction is expected to close in Q3, 2004 and is subject to SEC review and shareholder approval of both companies.

Source: [http://biz.yahoo.com/prnews/040603/dcth014\\_2.html](http://biz.yahoo.com/prnews/040603/dcth014_2.html)

24. *June 02, Associated Press* — **California's public health system unprepared for bioterrorism.** A think tank study has concluded that California's local health systems are not adequately prepared for bioterrorism attacks and major disease outbreaks. The study conducted by the Rand Corp.'s Health Center for Domestic and International Health Security examined the health departments in Los Angeles, Sacramento, Riverside, Imperial, Kern, and Del Norte counties, as well as the Berkeley health department, and found that some areas do not have the minimum capabilities to handle such attacks. **The report found "widespread variation" among local public health systems in their ability to protect the public from infectious**

**disease outbreaks and other public health threats.** Researchers simulated smallpox outbreaks to examine how well-equipped the target areas were to handle infectious disease outbreaks and bioterrorism attacks. **According to the study, there are no national standards for a public health system's preparedness for an infectious disease outbreak or a bioterrorism attack.** The seven counties examined in the study constitute about 40 percent of California's population.

Source: [http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern\\_california/8821930.htm?1c](http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/8821930.htm?1c)

[[Return to top](#)]

## **Government Sector**

25. *June 03, General Accounting Office* — **GAO-04-82: Overstay Tracking: A Key Component of Homeland Security and a Layered Defense (Report).** Published May 21. Each year, millions of visitors, foreign students, and immigrants come to the United States. The majority of visitors who are tracked depart on time, but others overstay — and since September 11, 2001, the question has arisen as to whether overstay issues might have an impact on domestic security. **In this report, the General Accounting Office (GAO) (1) describes available data on the extent of overstaying, (2) reports on weaknesses in the Department of Homeland Security's long-standing overstay tracking system, and (3) provides some observations on the impact that tracking system weaknesses and significant levels of overstaying may have on domestic security.** GAO provided a draft of this report to the Department of Homeland Security and the Department of Justice. Both agencies informed GAO that they had no comments. Highlights: <http://www.gao.gov/highlights/d0482high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-82>

26. *June 03, CNN* — **CIA chief Tenet resigns. CIA Director George Tenet has resigned, citing personal reasons,** President Bush said Thursday, June 3. Bush told reporters Thursday that Tenet had done "a superb job for the American people." Tenet said his resignation is effective July 11 — the seventh anniversary of his tenure in office. **In that time, he has led the CIA through the 1999 conflict in Kosovo, the al Qaeda attacks on New York and Washington and the wars in Afghanistan and in Iraq.** Deputy CIA Director John McLaughlin will become the agency's acting chief once Tenet steps down, Bush said  
Source: <http://www.cnn.com/2004/ALLPOLITICS/06/03/tenet.resigns/index.html>

[[Return to top](#)]

## **Emergency Services Sector**

27. *June 03, Palm Beach Post (FL)* — **Florida county SWAT teams unite for mock crises. More than 100 SWAT team members from three police departments worked together to handle simulated emergencies Wednesday, June 2, at Boca Raton, FL, Airport, marking a first for the agencies.** As FBI and Transportation Safety Administration officials observed, officers from Boca Raton, Delray Beach and Boynton Beach police departments, with Boca Raton Fire Rescue, worked in tandem to handle a bomb threat and a fake hijacker who had taken a hostage.

"It's a bigger, busier airport, and unfortunately, we live in a time when we have to be prepared for anything," Boca Raton police spokesperson Jeff Kelly said. The training session also came in handy for the departments' bomb-sniffing dogs. Everyone involved had to get used to working in full gear in sweltering heat.

Source: [http://www.palmbeachpost.com/localnews/content/auto/epaper/editions/thursday/south\\_county\\_04ebb9317231104400c9.html](http://www.palmbeachpost.com/localnews/content/auto/epaper/editions/thursday/south_county_04ebb9317231104400c9.html)

28. *June 03, McKinney Messenger (McKinney, TX)* — **Four agencies receive homeland security grants.** More than \$1.1 million in new federal grants will be helping Collin County, TX, law enforcement officials fight crime and terrorist attacks at home. Homeland security and law enforcement terrorism prevention grants will help Collin County and the cities of Allen, McKinney, and Plano to purchase new equipment. Homeland security grants are aimed at improving intelligence, warning communication systems and facility security. **The 2004 Law Enforcement Terrorism Prevention Program's \$201,332 will fund planning, intelligence distribution networks, equipment and training. Distribution of the two grants is based on different formulas. Population is a key criterion for homeland security, while perceived threat is used for law enforcement funds.** In most cases, the agencies received funds for specific equipment, plus regional money, for specific projects. "Southlake is part of a 14-city consortium that has been working together a long time," said Greg Dawson, emergency preparedness programs director for the North Central Texas Council of Governments. Source: [http://www.zwire.com/site/news.cfm?newsid=11849917&BRD=1426&PAG=461&dept\\_id=528204&rft=6](http://www.zwire.com/site/news.cfm?newsid=11849917&BRD=1426&PAG=461&dept_id=528204&rft=6)
29. *June 03, Associated Press* — **Emergency response drill on Long Island. Residents and business owners across Long Island will be encouraged to participate in what has been billed as a first-ever island-wide drill next week to test emergency response preparations in the event of a blackout, terrorist attack or natural disaster, Gov. George Pataki said Thursday, June 3.** Coordinated by the Long Island Power Authority (LIPA) and the state's Emergency Management office, the drill next Thursday will include fire departments from across the island, as well as the emergency management personnel from both Nassau and Suffolk counties, and New York City. LIPA officials are asking customers to cut their electric use between noon and 3 p.m. on that day to simulate conditions that might happen after a hurricane or during a blackout. He made the announcement during a two-day conference of approximately 500 first responders and other emergency services personnel from Long Island and New York City. "We were ready to respond to last year's August blackout immediately, because we took the time over the years to plan, prepare and drill," said LIPA chairman Richard Kessel. Source: [http://1010wins.com/topstories/winstopstories\\_story\\_15515394\\_3.html](http://1010wins.com/topstories/winstopstories_story_15515394_3.html)
30. *June 02, General Accounting Office* — **GAO-04-612: Wildfire Suppression: Funding Transfers Cause Project Cancellations and Delays, Strained Relationships, and Management Disruptions (Report).** In 2003, wildfires burned roughly four million acres, destroyed over 5,000 structures, took the lives of 30 firefighters, and cost over \$1 billion to suppress. To pay for wildfire suppression costs when the funds appropriated are insufficient, the U.S. Forest Service and the Department of the Interior have transferred funds from their other programs. The General Accounting Office (GAO) was asked to identify (1) the amount of funds transferred and reimbursed for wildfire suppression since 1999, and the programs from which

agencies transferred funds; (2) the effects on agency programs from which funds were taken; and (3) alternative approaches that could be considered for estimating annual suppression costs and funding wildfire suppression. **GAO recommends several measures to minimize the impacts of funding transfers and to improve the estimates on which the agencies base their wildfire budgeting requests. Further, GAO is asking the Congress to consider alternative approaches for funding wildfire suppression.** In commenting on the draft report, Forest Service and Interior generally agreed with the report's findings and recommendations. Highlights: <http://www.gao.gov/highlights/d04612high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-612>

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

31. *June 04, CNET News.com* — **Groups debate wireless spectrum plans.** Representatives of the Federal Communications Commission (FCC), the Wireless Communications Association International (WCA) industry group and others spoke Thursday, June 3, in Washington, DC, during a panel discussion on the FCC's plans to streamline spectrum use. The federal agency has been looking to promote the use of wireless technology as a third viable broadband option to cable and DSL (digital subscriber line) service, as it tries to meet President Bush's bold challenge to make high-speed Internet access available to all Americans by 2007. Radio spectrum is a finite resource that the agency is looking to more efficiently manage. The FCC is expected to discuss and possibly vote on the proposed management of spectrum in the 2.5GHz to 2.69GHz range at its monthly meeting on June 10. **FCC commissioners and others have expressed concern that the spectrum has been underutilized. Furthermore, current spectrum licensees fear that their spectrum might be taken away. Some licensees agreed that the spectrum has not been used to its fullest potential but said regulations have limited them.**  
Source: [http://news.com.com/Groups+debate+wireless+spectrum+plans/2100-1034\\_3-5225845.html?tag=nefd.top](http://news.com.com/Groups+debate+wireless+spectrum+plans/2100-1034_3-5225845.html?tag=nefd.top)
32. *June 03, The Register* — **Opera update plugs vulnerability. Opera has updated its browser to prevent its software from being manipulated by would-be fraudsters to display a fake address to surfers.** A flaw in the "Shortcut Icon" feature of versions of Opera prior to 7.51 made it possible for phishers to fool users into believing that they are in a domain they trust (their bank, web-mail, etc.) while serving and receiving content in a hostile domain. The vulnerability opened up a mechanism for identity theft, credit card scams and more, according to security researchers GreyMagic Software. GreyMagic informed Opera of the vulnerability on May 19. A new version (7.51) was released Thursday, June 3, to address the problem.  
Source: [http://www.theregister.co.uk/2004/06/03/opera\\_cuts\\_phishing/](http://www.theregister.co.uk/2004/06/03/opera_cuts_phishing/)
33. *June 03, Associated Press* — **India's software exports estimated at \$12.5B. India's revenues from exports of software and back-office services grew more than 30 percent during the fiscal year that ended in March,** a trade group said Thursday, June 3. Those revenues stood at \$12.5 billion in the latest fiscal year, compared with \$9.6 billion in the previous year, Kiran Karnik, president of the National Association of Software and Service Companies said. **U.S. companies continued to be the main source for India's outsourcing industry, accounting**

**for 70 percent of its revenues.** Revenues from back-office services that include call centers and documentation companies grew faster than from software development. Software revenues grew 25 percent to \$8.9 billion, while back-office revenues grew 46 percent to \$3.6 billion. Most large American companies have software development or routine office functions such as customer services or payroll documentation done in countries such as India, where wages and costs are much lower. While a number of U.S. states are considering bills to restrict outsourcing, Karnik said he expects India to see revenue growth of 30 percent to 32 percent in the current fiscal year.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12645-2004Jun 3.html>

- 34. June 03, Federal Computer Week — OMB tweaks info security rules.** The House Government Reform Committee's Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee asked federal and industry officials to testify Wednesday, June 2, at a hearing on the growing threat of network vulnerabilities. Karen Evans, administrator for electronic government and information technology at the the Office of Management and Budget (OMB) told lawmakers the revised guidelines will require agency officials and each agency inspector general to vouch that systems are configured to the minimum-security standards they cite in their FISMA reports. In other testimony Amit Yoran, director of the Department of Homeland Security's (DHS) National Cyber Security Division said DHS is formalizing its relationships with federal, state and local government agencies, academic institutions, industry groups and businesses through a new effort called the United States Computer Emergency Readiness Team (US-CERT) Partner Program. Through the program **DHS officials plan to create a permanent control-system center for collecting, analyzing, sharing and responding to cybersecurity threat information. Yoran said the control center and a related testing facility will be used to protect the computer and network systems that control the nation's critical infrastructure, which includes power grids, dams and water filtration systems.**

Source: <http://fcw.com/fcw/articles/2004/0531/web-omb-06-03-04.asp>

- 35. June 02, InternetNews.com — Security bug in Linksys Wireless-G Router.** A security bypass flaw in a popular wireless broadband router shipped by Cisco's Linksys unit could give malicious hackers administrative access to vulnerable devices, researchers warned on Wednesday, June 2. Independent technology consultant Alan W. Rateliff discovered the flaw during a client installation of a Linksys WRT54G Wireless-G Broadband Router and reported it to Linksys. According to Rateliff, **even if the remote administration function is turned off, the router provides the administration Website to ports 80 and 443 on the WAN.** "Out of the box the unit gives full access to its administration from the WAN using the default or, if the user even bothered to change it, an easily guessed password," he said. Security consultants Secunia rates the flaw as "moderately critical" and urged users to configure a strong password for the administrative Web interface or restrict access to the interface altogether. As a workaround until a firmware upgrade is issued, Rateliff recommends the use of port forwarding send ports 80 and 443 to non-existent hosts.

Source: <http://www.internetnews.com/infra/article.php/3362321>



### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**Watch Synopsis:** 3PM Update There is a new Worm called Plexus that exhibits many of the same characteristics that MyDoom exhibited. The initial variant does not target federal or military systems, but we can be certain that future variants may do so. This worm appears to be a blended threat and propagates by at least 5 various methods.

### Current Port Attacks

<b>Top 10 Target Ports</b>	445 (microsoft-ds), 135 (epmap), 1026 (nterm), 1027 (icq), 139 (netbios-ssn), 1025 (blackjack), 5000 (BackDoorSetup), 2745 (Bagle.C), 137 (netbios-ns), 1434 (ms-sql-m) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## General Sector

**36. *June 03, Scotsman (United Kingdom)* — Dirty bomb attack a growing risk. A rise in the level of smuggling of radioactive material has increased the risk of a dirty bomb attack by terrorists, atomic experts warned Wednesday, June 2.** Evidence from the United Nations' International Atomic Energy Agency (IAEA) shows there were 51 smuggling incidents last year compared with just eight in 1996. Most cases are believed to have occurred in Russia and elsewhere in Europe. Smugglers looking for radioactive materials target factories, hospitals, and research laboratories, which are not guarded as securely as nuclear industry facilities. The growing problem was highlighted in released IAEA records. **They disclosed that since 1993 there had been 300 confirmed cases of illicit trafficking in radiological materials, 215 of them in the last five years.** The IAEA warned that the real level of smuggling might be significantly higher, citing reports of a further 344 instances over the past 11 years which have not been confirmed. Radiological materials are radioactive sources that can be used in dirty bombs but not in nuclear-blast weapons. A dirty bomb is designed to spread radioactive material by combining it with conventional explosives.

Source: [http://thescotsman.scotsman.com/international.cfm?id=6300820\\_04](http://thescotsman.scotsman.com/international.cfm?id=6300820_04)

[[Return to top](#)]

## **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

**DHS/IAIP Alerts** – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

**DHS/IAIP Daily Open Source Infrastructure Reports** – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues.

**DHS/IAIP Daily Reports Archive** – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.